

Assessment form submitted by Nazmiye SAĞLAM for Ahi Evran imam Hatip Ortaokulu -
06.11.2019 @ 20:36:26

Infrastructure

Technical security Pupil and staff access to technology

Question: What is the pupil/computer access in your school?

- > **Answer:** There are specific computer labs, which can be booked by the teacher and the teachers make good usage of this option.

Data protection

Question: How is the storage of school records and other documentation dealt with over time?

- > **Answer:** We have a school retention plan specifying how long specific kinds of records are being kept and how they should be archived/disposed of.

Question: How is pupil data protected when it is taken 'off site' or being sent by email?

- > **Answer:** Our email system is protected with passwords and firewalls, and we have rules in place about the transfer of pupil data.

Question: Do you consistently inform all school members about of the importance of protecting devices, especially portable ones?

- > **Answer:** Yes, we provide training/manuals around issues like these.

Question: How are staff and pupil passwords generated for access to your school system?

- > **Answer:** New users are given a standard password and asked to generate their own password on their first access.

Software licensing

Question: Does someone have overall responsibility for licensing agreements?

- > **Answer:** Yes.

Question: Has the school set a realistic budget for the software needs?

- > **Answer:** Yes.

IT Management

Question: What happens if a teacher would like to acquire new hard/software for the school network?

- > **Answer:** Once a year we have a staff meeting where decisions about new hard/software are made.

Question: Are teachers and pupils allowed to install software to computers that are school property?

- › **Answer:** No, this can only be done by the person in charge of the school ICT network.

Question: Once new software is installed, are teachers trained in its usage?

- › **Answer:** Yes, when we roll-out new software, training and/or guidance is made available.

Policy

Acceptable Use Policy (AUP)

Question: Are eSafety issues referred to in other school policies (e.g. behaviour, anti-bullying, child protection)?

- › **Answer:** Yes, eSafety is an integral part of several school policies.

Question: Does your school have an Acceptable Use Policy (AUP)?

- › **Answer:** Yes, there is an AUP which covers all members of the school community.

Reporting and Incident-Handling

Question: Does your school have a strategy in place on how to deal with bullying, on- and offline?

- › **Answer:** Yes, we have a whole-school approach, addressing teachers, pupils and parents. It is also embedded into the curriculum for all ages.

Question: Is there a clear procedure if pupils knowingly access illegal or offensive material at school?

- › **Answer:** Yes. This is included in written guidance for staff.

Question: Is there a procedure for dealing with material that could potentially be illegal?

- › **Answer:** Yes.

Question: Does the school take any responsibility for any online incidents that happen outside the school?

- › **Answer:** No.

Staff policy

Question: What happens to a teacher's account once s/he changes her/his role or leaves the school?

- › **Answer:** The administrator is informed and immediately deactivates the teacher account or adjusts rights where possible.

Pupil practice/behaviour

Question: Is there a school wide hierarchy of positive and negative consequences to address pupils' online behaviour?

- › **Answer:** Yes and this is clearly understood by all and applied consistently throughout the school.

Question: When discussing eSafety related aspects, do pupils have the possibility to shape (extra-curricular and curricular) school activities based on what is going on in their daily lives?

- › **Answer:** Pupils are actively encouraged to choose topics of their interest and/or shape extra-curricular activities.

School presence online

Question: Does the school have an online presence on social media sites?

> **Answer:** Yes.

Practice

Management of eSafety

Question: Is there one single person responsible for ICT usage and online access in your school?

> **Answer:** No, teachers are responsible for their pupils' use of ICT and their online safety and security.

Question: Does the school have a designated member of staff responsible for eSafety?

> **Answer:** It is a shared responsibility for all staff.

eSafety in the curriculum

Question: Do you talk about online extremism/radicalisation/hate speech as part of your online safety curriculum?

> **Answer:** Yes, we have integrated discussion and education about these issues into our curriculum.

Question: Is eSafety taught as part of the curriculum?

> **Answer:** Yes.

Extra curricular activities

Question: Does the school have any up-to-date information about the online habits of pupils?

> **Answer:** Yes, we have plenty of information.

Question: Do pupils do peer mentoring about eSafety?

> **Answer:** Yes, on a regular basis.

Sources of support

Question: Are other school services involved in eSafety issues (e.g. counsellors, psychologists, school nurse)?

> **Answer:** Yes, we have a lot of support from them.

Question: Does the school provide eSafety support for parents?

> **Answer:** Yes, regularly.

Staff training

Question: Are teachers trained on the topic of cyberbullying?

> **Answer:** Yes, every teacher.

Question: Can teachers organise a training themselves if they have expert knowledge they would like to share with their colleagues?

> **Answer:** Yes, our school encourages knowledge exchange between staff members. There is also an online community which staff members use.